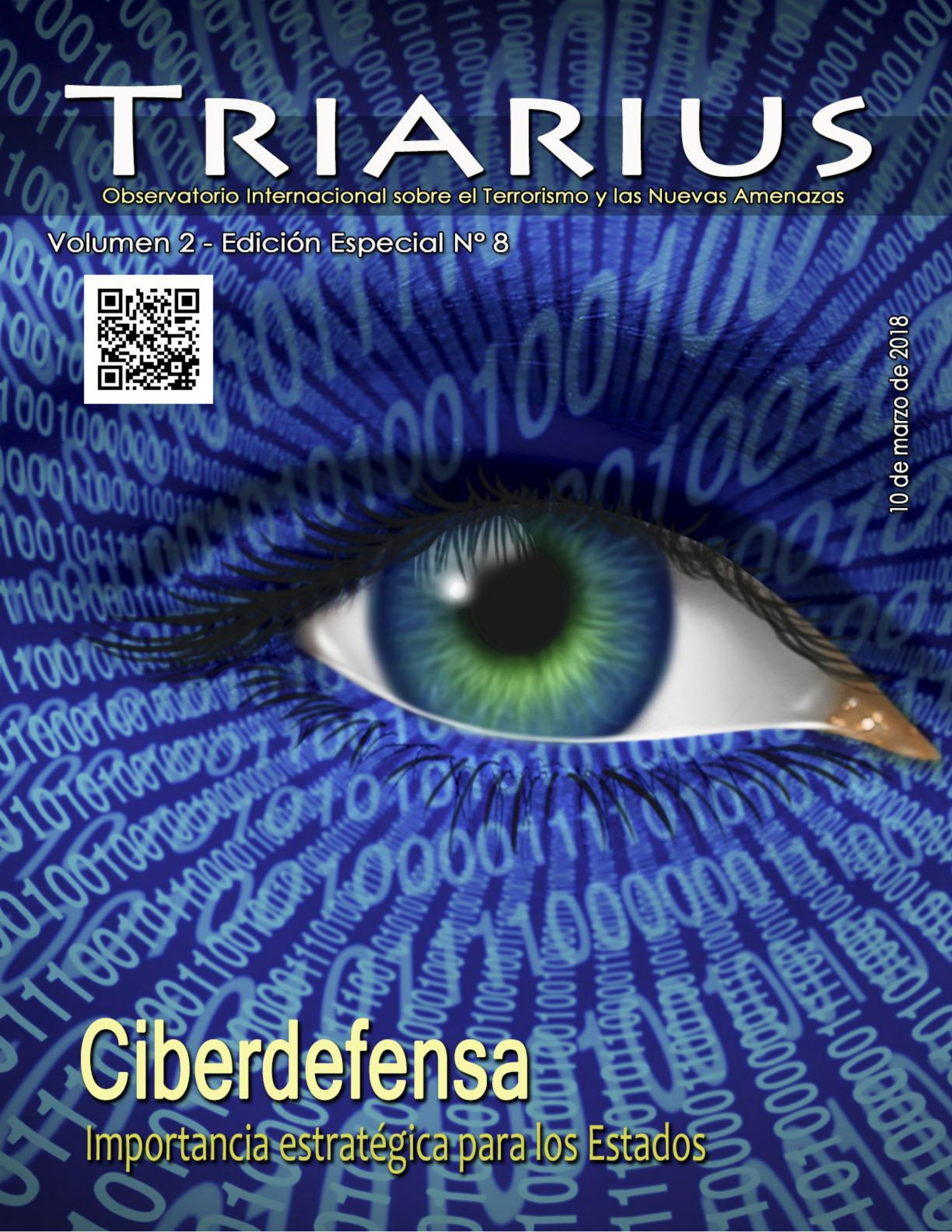
TRIARIUS

Observatorio Internacional sobre el Terrorismo y las Nuevas Amenazas

Volumen 2 - Edición Especial Nº 8

10 de marzo de 2018



Ciberdefensa

Importancia estratégica para los Estados

Medellín - Colombia
Edición Especial No. 8
10 de marzo de 2018

Editor
Douglas Hernández

Autor de esta obra
Joany Alonso Guerrero Herrera

Oficial Superior de grado Mayor (r), Magíster en Inteligencia Estratégica. Director Security College US en Colombia; CEO de le empresa Master Security Consulting, Gerente en la seguridad y analista sociopolítico; coautor del libro Inteligencia estratégica, el estado y la seguridad, estudios de caso; Docente de Ciberguerra, ciberseguridad y seguridad de la información; Máster en Seguridad de la información y consultor en seguridad privada.

Información de Contacto:

Douglas Hernández
Medellín, Colombia
Movil: (+57) 321-6435103
director@fuerzasmilitares.org
hernandez.douglas@hotmail.com

Presentación

El mundo moderno, globalizado e interconectado, presenta un increíble número de oportunidades en todos los campos, pero también un sin número de nuevas amenazas.

TRIARIUS, reconoce que las ciberamenazas constituyen un aspecto clave de la modernidad, al que hay que prestar toda atención. Por ello presenta este número especial dedicado a la ciberdefensa.

Hemos tenido la suerte de contactar al señor Mayor (r) Joany Guerrero, oficial retirado del Ejército Colombiano, con experiencia en las áreas de inteligencia, y particularmente en el tema de la Ciberdefensa, y hemos establecido lazos de cooperación de largo plazo, al entender que compartimos el objetivo de luchar contra el terrorismo -en todas sus manifestaciones- y contra las nuevas amenazas.

Este documento es apenas el inicio de una serie de colaboraciones orientadas a comprender las ciberamenazas y el ciberterrorismo, al tiempo que se abordan temas de ciberseguridad y ciberdefensa.

Esperamos sea de interés y utilidad para nuestros amables lectores.

¡Conocer para vencer!

Douglas Hernández
Editor

CIBERDEFENSA: IMPORTANCIA ESTRATÉGICA PARA LOS ESTADOS

Por Joany Alonso Guerrero Herrera

Resumen

El presente artículo presenta una revisión a la literatura concerniente a la necesidad que tienen los Estados para planear y desarrollar operaciones militares en el ciberespacio, lo cual representa grandes retos para la conformación de equipos multidisciplinarios alrededor de las nuevas tecnologías que diariamente avanzan en el área de las TIC[2], las cuales generan escenarios completamente diferentes dado el entorno en el que se conducen estas actividades, entendiendo que los actores, los medios y los métodos, son distintos a los ordinarios ya conocidos por los expertos en la defensa de Estado.

Para tal fin, las Fuerzas Armadas de los Estados han evolucionado de la mano de la empresa privada para controlar y generar diferentes maneras de abordar temas como el ciberterrorismo, el cibercrimen y las ciberamenazas (Gagnon, 2013), que diariamente forjan acciones que impactan la actividad política y económica de los Estados, sumado a la afectación a la seguridad de sus ciudadanos. De esta forma, se espera que el presente documento sirva como referente para los organismos de seguridad del Estado facultados para desarrollar operaciones en el ciberespacio, permitiéndoles hacer una valoración sobre si el fenómeno plantea o no, la necesidad de que en cada uno de ellos se conformen equipos compuestos por personal civil con experticia en informática avanzada, aun cuando ello podría exponer la compartimentación de las actividades de inteligencia propias de la seguridad nacional. Para tal fin, el documento esgrimió un método de revisión literaria de publicaciones de carácter científico, teniendo en cuenta una sucesión de criterios de búsqueda relativos al objeto de la investigación que fuesen pertinentes a la misma.

Palabras clave: Seguridad y defensa, Inteligencia Estratégica, Ciberguerra, Ciberseguridad, Cibercrimen, Operaciones Multinivel.

Abstract

This article presents a review of the literature concerning the need for States to plan and develop military operations in cyberspace, which represents major challenges for the formation of multidisciplinary teams around the new technologies that daily advance in the area of The ICTs, which generate completely different scenarios given the environment in which these activities are conducted, understanding that the actors, means and methods are different from the ordinary ones already known to experts in the defense of State.

To this end, the Armed Forces of the States have evolved from the hand of private enterprise to control and generate different ways of addressing issues such as cyberterrorism, cybercrime and cyber threats, nascent that daily forge actions that impact political and economic activity Of the States, added to the affectation to the security of its citizens. In this way, it is expected that this document serves as a reference for state security agencies authorized to develop operations in cyberspace, allowing them to make an assessment of whether or not the phenomenon raises the need for each of them Make up teams composed of civilian personnel with advanced computer skills, even though this could expose the compartmentalisation of national security intelligence

[2] Tecnologías de información y comunicaciones.

activities. To this end, the document proposed a method of literary revision of scientific publications, taking into account a succession of search criteria relating to the subject matter of the research that were relevant to it.

key words: Security and Defense, Strategic Intelligence, Cyberwarfare, Cybersecurity, Cybercrime, Multilevel Operations.

Introducción

A partir del año 2007 como lo mencionó Jacobson (2008) la OTAN y los Estados Unidos enviaron a un grupo de expertos informáticos a Estonia para que ayudarán a esta nación a reponerse de unos ciberataques recibidos, los cuales hoy día nadie se atribuye. El impacto que generó en este país un ataque de denegación de servicio sobre las comunicaciones, páginas del gobierno y el sector bancario, puso en evidencia la fragilidad que tienen los Estados para enfrentar las nuevas amenazas en el ciberespacio.

Sin embargo, el ejemplo anterior no ha sido la única acción que ha permitido constatar cómo la seguridad nacional de un país puede verse comprometida a través de una acción denominada "virtual", como lo relato Cymerman (2010):

> Irán sufrió el 27 de septiembre de 2010 de confirmarse, el ataque cibernético más grande de la historia. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se vieron afectados por un virus de una potencia sin precedentes, denominado Stuxnet. Los expertos consultados afirman que el 60% de los ordenadores iraníes se podrían haber visto afectados, igual que el 20% en Indonesia y el 8% en India. (p.16)

A raíz de estos primeros ataques de gran escala, la mayoría de Estados a nivel mundial se han venido preparando con el ánimo de reaccionar ante este tipo de acciones bélicas. De esta manera, países como España y Estados Unidos particularmente han creado centros de respuesta a incidentes informáticos y comandos de Ciberdefensa.

Por su parte, Colombia, luego de publicar el Ministerio de las TIC (2011), MinTic, el documento CONPES 3701 sobre los *Lineamientos de Política para Ciberseguridad y Ciberdefensa*, se ha venido preparando el gobierno en esta materia con avances significativos en gestión documental, sensibilización y difusión de normativas. Sin embargo, se ha hecho evidente que las capacidades de reacción y desarrollo e investigación, son limitadas, dado que las personas que dirigen estos equipos de trabajo no cuentan con capacitación técnica y experiencia en estos campos, considerando la existente rotación permanente del personal en los organismos de seguridad del Estado. Es en este punto, donde surge la inquietud sobre si este componente de seguridad nacional debería ser o no, integrado también por personal civil con capacidades técnicas, aun cuando no tienen formación y disciplina militar.

Metodología

Para el desarrollo de este artículo se realizó una búsqueda de literatura concreta en materia de ciberguerra, preparación de los Estados para enfrentar amenazas en el ciberespacio, Ciberseguridad y estrategia aplicada a guerra asimétrica, en los catálogos de la biblioteca del buscador Google Scholar, Scopus y Scielo, que permiten realizar búsquedas especificas en la web a partir de editoriales, bibliotecas, repositorios, bases de datos bibliográficas, entre otros; y entre sus resultados se pueden encontrar libros, artículos de revistas científicas, y tesis. Con la finalidad de realizar una revisión amplia y actual del objeto de estudio.

Amenazas que enfrentan los Estados en el ciberespacio

Para abordar este escenario primero hay que hacer una contextualización sobre los riesgos o amenazas que enfrentan los Estados en el ciberespacio. Para tal fin, la Real Academia Española RAE (s.f) definió al ciberespacio como el ámbito artificial creado por medios informáticos" (párr. 1). Sin embargo, esta definición es ambigua y tiene una profundidad reducida, teniendo en cuenta que en la actualidad se observan interacciones abismales en este complejo dominio, como lo menciono Parra & Mena (2014) hay una relación permanente entre lo físico y lo virtual como movimientos sociales y protestas que impactan la geografía pero que se organizan en lo virtual. No obstante, esta definición no tiene en cuenta la comunicación creada a través de las redes sociales por diferentes actores en el ciberespacio, fenómeno estudiado por Christakis & Doler (2010) haciendo alusión al concepto de la *multiplexidad* para explicar la influencia de las redes sociales en los comportamientos de las personas.

Ahora bien, el MINTIC (2011) hizo referencia al término, ecosistema digital, identificando en él cuatro elementos que interactúan entre sí y que son necesarios para que exista un ciberespacio: primero, la infraestructura compuesta por equipos informáticos como dice (Caruso & Masters, 2014) routers, switchs, redes LAN, servidores, celulares, televisores, neveras, vehículos, marcapasos, relojes, impresoras, computadores, GPS, aviones, cámaras de seguridad, semáforos, redes SCADA, cableado etc; segundo, el servicio donde confluyen todas las actividades que se realizan a través de la interacción con la infraestructura, como las llamadas telefónicas, el internet, la navegación a través de un GPS, la visualización de imágenes mediante una página web, etc; Tercero, las aplicaciones que permiten la conexión y la transformación de una infraestructura en un servicio cómodo y agradable, como lo son la banca móvil, Facebook, YouTube, programas de sistematización de geolocalización, etc.; Por último, los usuarios, llámense personas u organizaciones de todo nivel, empresas, instituciones o gobiernos.

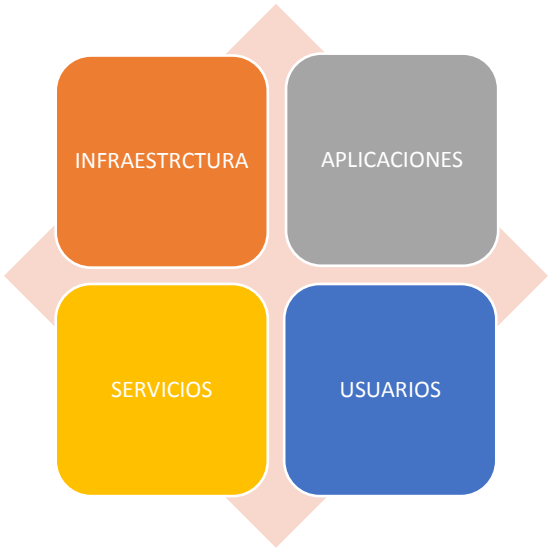


Figura 1. Figura elaborada por el presente autor del artículo con base en la información de MINTIC (2011)

La interacción de los elementos anteriormente mencionados genera una gran revolución entre los componentes que permanentemente se comunican entre sí, transmitiendo todo tipo de datos mediante distintos protocolos, provocando una explosión de información circulante, como lo afirmo García (2005, p. 334) "de un modo más general, cabe señalar que la digitalización ha promovido una serie de avances tecnológicos cuya

importancia deviene de las mutaciones que provocan en el conocimiento de los individuos, su intercomunicación y representación en la cibersociedad”

> De este modo, los conceptos mencionados, evidencian que el ecosistema digital se incrementa de manera exponencial derrumbando fronteras, generando además de nuevo conocimiento, grandes riesgos en la seguridad de los Estados. Por tanto, luego de evidenciar la posición de los Estados al interior del ecosistema digital o ciberespacio, se determina cuáles son las reales amenazas que enfrenta la seguridad nacional. Para ello, Quigley, Burns, & Stallard (2015) Expusieron que los grandes especialistas de la seguridad cibernética, aportan más en la difusión de los problemas que se presentan en la red, que en las mismas soluciones, sin embargo su investigación permite detectar que los gobiernos identifican cuatro grandes riesgos que deben enfrentar cuando a ciberespacio se refiere: el hacktivismo, los delitos cibernéticos, el ciberterrorismo y la guerra cibernética. (Jordan & Taylor, 2004).

Para presentar un concepto de hacktivismo se dice que “Las palabras "hacker" y "activismo" podrían sugerir: la idea de promover o resistir algún tipo de cambio político o social a través no violentos pero a menudo cuestionables medios de protesta cibernéticos.” (Singer & Friedman, 2014, p. 77), por otro lado define el cibercrimen como “el uso de herramientas digitales por delincuentes para robar o de otra manera llevar a cabo actividades ilegales” (Singer & Friedman, 2014 p. 85)

Precisamente, es en este punto donde surge una de las grandes diferencias con relación a la forma cómo los Estados y la industria enfrentan este tipo de amenazas, considerando que por parte de los gobiernos las estrategias de defensa nacional a menudo han hecho una interpretación de los riesgos en términos de su capacidad para resistir un ataque de un enemigo, entendiendo su naturaleza, en búsqueda de la supervivencia del Estado; por otra parte, en la industria los riesgos se miden en pérdidas y ganancias y en lugar de pensar en ciberinteligencia, espionaje o guerra cibernética, su objetivo es la prevención de fraudes, protección de marca, evitar el espionaje industrial, custodiar la propiedad intelectual, responsabilidad y protección de marca.

Figura 2. Figura elaborada por el presente autor del artículo con base en la información (Quigley et al., 2015)

De acuerdo con Quigley et al (2015) el panorama identificado en el ciberespacio presenta además varios aspectos que abren la discusión con respecto a otros autores, por ejemplo una de las propuestas analizadas por estos autores, es que debe haber cooperación entre la industria y el sector gubernamental para el diseño de una estrategia en Ciberdefensa efectiva que traiga consigo resultados óptimos o por lo menos aceptables. Como menciona lo Caro (2010):

> “El ciberespacio ha experimentado un enorme y veloz desarrollo, así como la dependencia que nuestra sociedad tiene de él, lo que contrasta con el menor y lento avance en materias de ciberseguridad. Por este motivo, los actores (tanto estatales como no estatales) que decidan operar en el ciberespacio, obtendrán una serie de ventajas asimétricas, como son las siguientes: – El ciberespacio es un «campo de batalla» de grandes dimensiones y donde resulta relativamente fácil asegurar el anonimato. Los ataques se pueden lanzar desde casi cualquier parte del mundo. – Los efectos de los ataques son desproporcionados con respecto a su coste. Las operaciones se pueden realizar sin necesidad de efectuar fuertes inversiones en recursos humanos y materiales. – La naturaleza de los ciberataques fuerza a la mayoría de las víctimas, tanto reales como potenciales, a adoptar una actitud defensiva. – Esta amenaza tiene un alcance global, en la cual el actor (ya sea ciberdelincuente, ciberterrorista, etc.), puede operar desde cualquier parte del mundo con el único requisito de tener acceso al ciberespacio. La conexión al ciberespacio de cualquier sistema lo convierte en un objetivo susceptible de ser atacado.” (p.52)

Existen ejemplos de cooperación entre instituciones del Estado y personal civil o llamados contratistas como lo describe Scheuerman (2014) en donde un contratista que trabajaba para la NSA termina revelando información clasificada acerca de métodos y procedimientos utilizados por la agencia estadounidense para obtener información a través de la red, se llega a un punto de no retorno donde si bien es cierto que el sector privado tiene grandes recursos a nivel tecnológico y técnico, como lo sugirió Quigley et al. (2015) en su análisis del factor riesgo, no es el mismo que tiene el Estado aun cuando en algunos puntos pueda ser muy parecido, esto conlleva a repensar como se podría estructurar esta alineación de esfuerzos, dado que como lo afirmó Elliott, Massacci & Williams (2016) este tipo de actividad es de difícil cuantificación y las empresas que le apuesten a este tipo de alianza en pro de la seguridad y defensa de un Estado, debe recibir un retorno de su inversión que permita entender este esfuerzo como una inversión y no como un gasto.

Por otro lado, la posición de los Estados frente a la seguridad en el ciberespacio va tomando protagonismo en sus estrategias de seguridad y defensa, tal es el caso de la Unión Europea y la OTAN donde en su estrategia global dan relevancia a estos fenómenos.

> Además de destacar los logros de la Unión en temas de seguridad desde la publicación de la primera estrategia, se ponen al día los acontecimientos relevantes, se mantiene la visión general, se confirman los retos y amenazas que enfrenta la Unión y se añaden al listado los ámbitos de la ciberseguridad, la seguridad energética y el cambio climático. (García, 2016, p.34)

Aunado a esta situación, se observan temas tan variados que afectan estas nuevas amenazas y que implican una manera de repensar como se abordan estos riesgos por parte de los Estados, por ejemplo Armstrong, Kleidermacher, Klonoff, & Slepian (2016) fijan un punto de partida poco explorado y de gran impacto en la sociedad como lo es la amenaza latente en los dispositivos médicos con tecnología de conectividad, donde identifican como un paciente de diabetes que lleva consigo un dispositivo electrónico capaz de medir los niveles aceptables de azúcar en la sangre para su correcto tratamiento y control, por el solo hecho de emplear tecnología compuesta de software y hardware tiene vulnerabilidades que eventualmente podrían explotar y generar daños contra la disponibilidad, la confidencialidad e incluso la integridad de la información que lleva consigo.

Cyberhuman

Además de describir los grandes retos para la seguridad en este escenario del ciberespacio, se presentan actores que convencionalmente no se tenían en cuenta como protagonistas en la seguridad y defensa nacional. De acuerdo con Enamorado (2013):

> En la práctica, los diferentes actores que usan el ciberespacio se encuentran a milisegundos unos de otros, lo que explica que en este ámbito las distancias geográficas sean irrelevantes, dicha circunstancia incrementa el número de participantes en la ciberguerra, puesto que da acceso a nuevos actores. (p.333)

De hecho, hoy en día los riesgos de supervivencia de un Estado no solo conllevan a tener especial atención a países con algún tipo de interés geopolítico sobre el territorio de su propiedad, sino también personas, grupos hacktivistas, organizaciones ilegales y por qué dejar de un lado grandes corporaciones; como menciona Hurlburt (2015) el ser humano está en el centro de la discusión sobre la Ciberseguridad y acuña el término de cyberhuman como actor principal dentro del entramado que lleva todo un concepto de seguridad cibernética, haciendo un paralelo de como los Estados Unidos consideran su defensa a través de HUMINT, CIBERINT, DNINT, SIGINT, COMINT, ELINT, FISINT, TELINT, FININT, TECHIN, MEDINT, GEOINT, IMINT, MASINT y OSINT, todas ellas con un común denominador el cual es la interacción humana. Es decir, que la seguridad cibernética lleva un componente humano decisivo al momento de plantear maneras de enfrentar estas amenazas, dado que desde una mala configuración por parte de un especialista que deje vulnerable un servicio, hasta la producción de códigos maliciosos con el fin de generar indisponibilidad de una infraestructura crítica vital para la conservación de un Estado.

Por otro lado, y reforzando el concepto de cyberhuman presentado anteriormente, Strawser & Joy (2015) hace referencia a la percepción de responsabilidad de los usuarios presentado, donde se plantea que en la actualidad, cuando hay fuga de datos personales como fotografías intimas y documentos personales tales como claves de acceso, tarjetas de crédito y demás información confidencial, suele ser cuestionado el usuario como responsable, teniendo en cuenta el concepto de que al tener dicha información sensible se debe estar preparado para que sea vulnerada y expuesta, (Ruiz, 2002). Uno de los ejemplos que proponen para entender la responsabilidad de los usuarios, es que así como una persona debe proteger su casa con cerraduras, puertas y ventanas, de la misma forma debe protegerse la información, pasando a un punto de discusión clave donde se asume como normal y aceptable el riesgo a ser atacado por un delincuente informático. Sin embargo (Strawser & Joy, 2015) explican que,

> …el anterior modelo permite observar desde un punto social la discusión de lo moralmente aceptado en las sociedades modernas, cuando ocurre un delito informático terminando por culpar al dueño real de la información y no al delincuente, la clara demostración de este postulado se evidenció en el año 2010 donde el conocido evento como “the Fappening” donde delincuentes informáticos develaron la existencia de fotografías de diferentes figuras públicas de Hollywood desnudas, y en la sociedad se terminó juzgando y culpando a las víctimas como responsables dado que no debieron tener en su posesión este tipo de archivos, ya que deberían haber sido consientes que tarde o temprano serían hackeados y expuestos.

Otro concepto de valor que aportan Strawser & Joy (2015) a la discusión, es que en la seguridad tradicional resulta sencillo medir la efectividad de los controles implementados para prevenir el delito. Es así como si en el

hogar una persona decide proteger sus artículos de mayor valor adquiere una caja fuerte y simplemente protege sus objetos, sin necesidad de actualizar parches, cambiara la versión o realizar pruebas permanentemente.

Ciberdefensa de infraestructura crítica

Al hablar de Ciberdefensa se abre un abanico de posibilidades, y basados en las amenazas anteriormente observadas, como dice Caro B., (2010) el Estado debe prepararse para enfrentar técnicamente los incidentes que puedan causar daños irreparables. Sin duda, al hablar de la defensa estratégica en el ciberespacio no se puede dejar a un lado la infraestructura crítica. Dentro de ese marco, "las definiciones de la infraestructura crítica tienden a ser amplias. Las definiciones de "crítico" se refieren a la infraestructura cuya interrupción o destrucción podría causar daños catastróficos y de largo alcance. "Infraestructura" se refiere a los bienes tangibles e intangibles y para los sistemas de producción y redes. La cobertura sectorial de los programas tiende a ser muy amplia." (Gordon & Dion, 2008, p 5).

Si bien se intenta identificar y proteger infraestructura crítica, los esfuerzos son aislados y se dan de manera individual dado que la inversión en investigación para la mitigación de estos riesgos es proporcional a la incertidumbre que se percibe, por ejemplo Vega Baeza & Durán Medina (2013) mencionan tangencialmente que es bien sabido que el sector financiero hace grandes esfuerzos para proteger su infraestructura tecnológica. Sin embargo, por otro lado el Ministerio de Defensa de España (2011) explica que sectores como el minero, el de salud y el de la educación -entre otros- no tienen como máxima prioridad la protección de sus activos tecnológicos a través de centros de monitoreo y control.

No obstante, existen diferentes métodos de monitoreo, como dicen Chen & Janeja (2014) están diferentes modelos basados en la detección de anomalías que puedan identificar ataques inusuales y desconocidos normalmente basados en sistemas de detección de intrusiones de dos maneras, los que se encuentran basados en el mal uso o identificación basada en firmas, y la detección basada en anomalías. Cada uno tiene sus pro y sus contras frente a las amenazas en la red, por ejemplo, la primera opción presenta problemas en la detección de nuevos ataques con firmas desconocidas; por otro lado, la detección basada en anomalías realiza un análisis histórico de las actividades "normales" generando alertas cuando se presentan comportamientos diferentes. Este método es muy efectivo, sin embargo, genera muchas falsas alertas debido al cambio de comportamiento de los usuarios. Para ser más explícito y que sea de mayor comprensión para el lector, se pone como ejemplo una actividad rutinaria. Supóngase que el centro de mando y control de una unidad táctica transmite datos a través de una red controlada y permanentemente supervisada por un modelo basado en firmas, cuando un atacante intenta penetrar la seguridad mediante el uso de un software malicioso el cual lleva inmerso una firma que ha sido reportada por alguna casa de antivirus, el sistema detecta y reporta la intención maliciosa, es decir, que si dentro de la red controlada Juan Pérez que trabaja en la oficina de registro descarga un programa que lleva inmerso un troyano, será detectado por la red generando una alerta inmediata para ser tratado, cuando esta misma actividad sucede pero se tiene un sistema de control basado en anomalías, el sistema detecta que el software que se está descargando normalmente no se utiliza para las labores diarias, y dispara las alertas permitiendo controlar estas actividades.

En este ejemplo, si Juan descargara un software de administración nuevo y necesario para su labor, sería detectado como una anomalía, generando reporte y retardando sus actividades, sin embargo, su seguridad no se vería comprometida, por otro lado con el sistema basado en firmas, si el ataque llegara de un nuevo virus el

cual nunca ha sido utilizado, como explican Goel & Hong (2015), lograría su objetivo y no despertaría sospecha alguna en los sistemas de detección dado que su firma aun no estará reportada.

Uno de los grandes aportes que Chen & Janeja (2014) realizan es que con el fin de detectar ataques con mayor precisión y para construir un robusto sistema de detección, se necesita emplear estudios de diferentes áreas, incluyendo las nuevas tecnologías, habilidades de minería de datos, psicología del atacante y los comportamientos normales de usuarios, etc. Nunca es suficiente utilizar sólo un método para adaptarse a todas las situaciones.

Los patrones de intrusiones son de naturaleza compleja y los comportamientos humanos son impredecibles dice García Rosales (2015), pero es necesario esforzarse por descubrir los ataques más rápido y a costos más bajos.

Parafraseando a Valenzano (2014) el prevenir un ataque contra la infraestructura crítica implica varios aspectos diferentes, desde la evaluación de los riesgos para la selección de las políticas de seguridad adecuadas que deben implementarse en las organizaciones, Arias-Cabarcos, Marin, Palacios, Almenarez, & Diaz-Sanchez (2016) complementan señalando que la adopción de controles o contramedidas, la gestión de parches de seguridad y actualizaciones, y la detección y reacción a los incidentes es solo el inicio del proceso. Cada esquema de protección, sin embargo, no puede abstraerse de la disponibilidad de las políticas de control de acceso adecuadas y mecanismos que están en la base de toda la estructura de seguridad. Es así como nos demuestra que el control de acceso por sí sola no es suficiente para ofrecer protección frente a ataques maliciosos; De hecho, no es capaz de evitar que un atacante se haga pasar por un usuario legítimo y lleve a cabo acciones no deseadas en su lugar. Sin embargo, las políticas de acceso y su aplicación son necesarios como un bloque de construcción básico para implementar contramedidas eficaces en la infraestructura crítica.

Las subestaciones eléctricas que tienen inmersos sistemas de control, supervisión y adquisición de datos (SCADA), desde el año 2010 se han convertido en cuestiones de ingeniería urgente, así lo mencionan Chen & Janeja (2014) manifestando que el aumento de la complejidad e interconexión de sistemas SCADA las han expuesto a una amplia gama de amenazas de seguridad cibernética, que puede conducir a un daño físico grave. Esto nos permite evidenciar cómo la infraestructura crítica de un Estado está en su gran mayoría en manos de particulares. Geer (2014) nos dice que en los Estados unidos casi toda la Infraestructura Crítica está en manos de privadas y prestadores de servicios de internet, de los cuales dependen cada vez más, convirtiéndose en esenciales para la vida normal. La respuesta del gobierno a la creciente penetración de los servicios de Internet en manos privadas teniendo como punto de partida que no poseen en sí la Infraestructura Crítica, los que la administran pueden y serán obligados a convertirse en agentes del gobierno.

De hecho los escenarios de ataques cibernéticos a gran escala son alarmantes, Marrero Travieso (2003) dice que para los años 90 eran impensables y solo se podían observar en películas de ciencia ficción, hoy están al alcance de todos, observado diariamente a través de los incidentes reportados en el mundo. Kremer (2014) introduce un concepto que denomina “mentalidad de la seguridad” realizando una comparación desde la escuela de Copenhague como un concepto en permanente construcción, recogiendo a Bruce Schneier desde la seguridad como actitud profesional y Kaarlo Tuori con su concepto de seguridad y su efecto en la legislación no están aislados de prerrequisitos sociales, culturales e institucionales, aplicándolos al escenario del ciberespacio,

determinando finalmente que debe existir una correlación entre la preparación profesional, la legislación y la evolución permanente.

El autor escoge dos perspectivas para analizar la seguridad en el ciberespacio, primero realiza una mirada desde el punto de vista militar y posteriormente desde el punto de vista policial. En este punto describe como desde los dos vértices constituyen mentalidad de protección, operan en gran medida desde perspectivas profesionales, y se centran en amenazas construidas con amparo legal por separado. Kremer (2014) manifiesta que predominantemente lo que está amenazado es el Estado (nación) y las capacidades militares son la principal respuesta a esas amenazas. En consecuencia, la retórica de la autodefensa, la integridad territorial y la soberanía, juegan un papel importante en la justificación de las medidas intrusivas, agresivas, y desde un punto de vista legal. El derecho internacional proporciona varios de estos mecanismos. Tal retórica bélica es fácilmente identificada cuando se trata de amenazas percibidas en el ciberespacio y la guerra podría incluso ser tratada con medios y métodos de guerra tradicionales.

En Mayo 2011, los EE.UU. publicaron su Estrategia Internacional para el Ciberespacio, que establece:

> "Cuando sea necesario, los Estados Unidos responderá a actos hostiles en el ciberespacio como lo haría con cualquier otra amenaza a nuestro país. Todos los estados tienen el derecho inherente a la autodefensa, y reconocemos que ciertos actos hostiles llevados a cabo por el ciberespacio podrían obligar a acciones en el marco de los compromisos que tenemos con nuestros socios de tratados militares, nos reservamos el derecho de utilizar todos los medios necesarios, diplomáticos, informativos, militares y económicas, según corresponda y de conformidad con el derecho internacional aplicable, con el fin de defender a nuestra nación, nuestros aliados, nuestros socios, y nuestra intereses. Al hacerlo, vamos a agotar todas las opciones antes de la fuerza militar siempre que podamos; será sopesar cuidadosamente los costos y riesgos de la acción contra los costos de la inacción; y actuar de una manera que refleje nuestros valores y fortalezca nuestra legitimidad," (Presidencia de los Estados Unidos, 2011, p. 14)

Por otro lado, el Reino Unido ha creado una unidad cibernética conjunta incrustado en las estructuras militares que desarrollaran y utilizan una gama de nuevas técnicas, incluidas las medidas proactivas, para interrumpir las amenazas a la seguridad de la información; Incluso Finlandia con su Ministerio de Defensa, en el 2016 se planteó ser un precursor mundial en la preparación ante la amenaza cibernética y en la gestión de las perturbaciones causadas por estas amenazas.

Todos estos hechos muestran una comprensión militarista de las amenazas del ciberespacio. La amenaza es el atacante externo, el otro, "el enemigo, el otro estado que utiliza Ciber-guerreros para atacar a un Estado, la infraestructura civil y militar, al mejor estilo de la guerra fría donde pareciera una gran carrera armamentista que permita disuadir a sus adversarios a través de la conformación de cibersoldados que permitan defender su Infraestructura Crítica compuesta por tecnología de carácter civil y militar. Como menciona Lucky (2010) por supuesto que las amenazas podrían ser reales, tales como el espionaje, sabotajes a la infraestructura militar, y el robo de la tecnología siempre han sido parte de la guerra, y no es de extrañar que con la tecnología militar moderna se convierta en uno de los objetivos de guerra de mayor necesidad para demostrar poderío.

Se podría decir entonces, como lo menciona Kremer (2014) que no hay defensa cibernética sin capacidad de ataque cibernético y es aquí donde se presenta el punto de quiebre para la estructuración de una unidad de Ciberdefensa efectiva o una unidad de ciberpapel que doctrinariamente es eficiente pero en la práctica actúa como un león sin dientes.

Retos para la Ciberdefensa

Lo principal es enfrentarse a un actor diferente, que no necesita un espacio geográfico definido, más que una computadora o un dispositivo móvil conectado a la red, de igual manera el perfil de este tipo de personas permite que pasen desapercibidos en la sociedad.

> "Sin embargo, la Ciberseguridad debe plantearse no sólo desde el punto de vista de las amenazas sino también desde los retos que plantean. La implantación de políticas de ciberseguridad servirá no sólo para la Seguridad Nacional sino también para aumentar la eficiencia y rentabilidad de la industria y empresas del sector de la seguridad e incluso en una vertiente mucho más amplia de todos los sectores de la vida nacional que al tener aseguradas sus ciberdefensas podrán dedicarse, con tranquilidad, a sus negocios fundamentales (core) lo que redundará en el aumento de su productividad y beneficiará a sus empleados, clientes, socios, y, en general, a los grupos de interés." (Ministerio de Defensa de España, 2011)

Si bien las compañías prestadoras de servicio de internet podrían identificar la dirección IP de un atacante, existen diferentes métodos para enmascarar la dirección y ocultarse de los controles técnicos de manera sencilla y sin necesidad de un conocimiento avanzado. La red Tor es uno de los más efectivos y utilizados actualmente, como lo menciona Alonso (2014)[7].

Otros elementos que dificultan la lucha contra la Ciberdelincuencia son las técnicas utilizadas por estos sujetos, en su gran mayoría utilizan software libre, programas gratuitos que circulan por la internet sin control alguno, es normal encontrar foros donde se solucionan distintos tipos de problemas informáticos, así como podría "subcontratar" algún tipo de servicio, por lo general en redes como la deep web como nos ilustra Cuende (2011) [9].

Bitcoins se convierte en una moneda digital, absolutamente difícil de rastrear ya que no pasa por bancos, ni por controles de los Estados, lo que hace que este tipo de comercio de software maligno utilizado para el delito prolifere de manera gradual a medida que los delincuentes van evolucionando.

Hasta el día de hoy, ningún país ha aceptado que ha realizado algún acto de guerra a través del Ciberespacio, sin embargo en su gran mayoría se preparan para la defensa como lo dice Karatzogianni (2008), creando centros o comandos cibernéticos de defensa y respuesta a incidentes.

Torres Soriano (2011) nos dice "Se trata de un nuevo tipo de guerra en el que las acciones tanto ofensivas como defensivas adoptan la forma de lenguaje binario e impulsos electromagnéticos. A pesar de tratarse de acciones que tienen su existencia en el ámbito virtual de las redes de comunicación y transmisión de datos, sus efectos se hacen sentir en el mundo físico." (p.14) Es aquí donde la amenaza se convierte en prioridad para los Estados, ya que a través de ordenadores o sus equivalentes se puede generar actividades de gran connotación que podrían poner en peligro la seguridad de las Naciones, ataques a la infraestructura crítica podrían poner en riesgo grandes asentamientos de población.

---

[7] Chema Alonso Dr. en Seguridad Informática por la Universidad Rey Juan Carlos de Madrid, Ingeniero Informático por la URJC e Ingeniero Informático de Sistemas por la Universidad Politécnica de Madrid en conferencia TED https://www.youtube.com/watch?v=3G7tVt0DTS4

[9] Luis Iván Cuende Fundador de Asturix y Stampery Mejor programador europeo menor de 18 años en el certamen HackNow en entrevista para world hacking http://aminoapps.com/page/world-hacking/7604052/que-es-la-deep-web-y-bitcoin

Uno de los antecedentes históricos de este fenómeno se presenta en Estonia, un país con una democracia joven, que se ha preocupado por estar a la vanguardia en interconexión en todos los organismos del Estado como lo menciona Greathouse (2014), desde las elecciones, banca electrónica y servicios de banca móvil.

El primero de mayo de 2007, día de la fiesta nacional Rusa, se inicia un ataque coordinado sobre las páginas oficiales de Estonia mediante Defacement un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor, generando caos y confusión en los administradores de las redes. La segunda fase fue una operación de denegación de servicio, mediante el envío excesivo de peticiones a los servidores, técnica utilizada mediante bots que lograron cortar la disponibilidad de páginas bancarias, noticias y del estado. Esto terminó generando un ambiente de caos creando movimientos sociales en las calles de Estonia donde las personas de origen ruso generaron revueltas, produciendo anarquía y poniendo a tambalear el gobierno de turno; se pudo determinar el origen de estos ciberataques en Moscú, donde se evidenció que millones de ordenadores intentaban conectarse a cualquier servidor en Estonia. El único recurso para su defensa fue el cortar los servicios de internet de todo el país, dejando fuera de línea todas sus instituciones y organizaciones privadas como públicas. Aquí se pudo evidenciar que un Ciberataque tiene varias fases y diferentes objetivos, como tal en Tallin -capital de Estonia-, se generó desorientación, confusión y caos a través de los medios informáticos. Pero igual manera un ataque puede tener un fin específico como el caso de Stuxnet que logró penetrar en los servidores de los reactores nucleares Iraníes, generando fallos en la red escada.

Por primera vez en el mundo se habla de *ciberarmas*, como lo explica Caro (2010) palabra que describe el software o el conjunto de software capaz de interrumpir, denegar o engañar un activo tecnológico, dependiendo su objetivo se podría diferenciar algunos tipos de ciberarmas. Pero, ¿dónde conseguir una ciberarma? Estos programas llamados virus, malware, scripts son fácilmente encontrados en diversos lugares de la red, también existen los llamados “0 days” que son fallos aun no reportados, a la venta del mejor postor (Clarke, 2010).

> “Numerosos países están estableciendo políticas de ciberseguridad. Así Gran Bretaña ha creado el GCHQ, un centro de operaciones equivalente de la NSA (National Security Agency) estadounidense. Ian Lobban, director del GCQH en un discurso pronunciado el 26 de octubre de 2010 pronunció las siguientes palabras: «Los países ya están usando técnicas de guerra cibernética para atacarse entre sí y necesitan estar alerta en todo momento para proteger los sistemas informáticos. El ciberespacio se disputa cada día, cada hora, cada minuto, cada segundo. La expansión del ciberespionaje ha elevado el riesgo de interrupción de infraestructuras como estaciones eléctricas y servicios financieros. La amenaza es real y creíble». Lobban en este discurso planteaba la existencia real de peligros en el ciberespacio.” (Ministerio de Defensa de España, 2011, p. 31)

Pero cuando hablamos de guerra entre estados, las aplicaciones son específicas y llevan detrás de su creación largas horas de programación y en muchos casos equipos gigantescos de desarrolladores. La guerra Cibernética o Ciberguerra tiene unas características especiales que la convierten en una amenaza mundial, donde cualquier Estado podría convertirse en actor directo o indirecto, sin importar su posición geográfica o su situación económica.

Para entender el anterior planteamiento a continuación se describen algunas características típicas de la Ciberguerra que sirven de combustible para la proliferación de acciones militares cibernéticas que nos describe detalladamente Torres Soriano (2011).

Bajo costo económico

Aun cuando la creación de una Ciberarma podría demorar meses o incluso un par de años de investigación, el modelado y ejecución de una Ciberarma bien concebida, con un objetivo específico será mucho menor al sostenimiento de un Ejército (Ministerio de Defensa de España, 2011). Teniendo en cuenta que la preparación de unas fuerzas militares para la guerra, trae consigo unos costos diferenciales desde la etapa de entrenamiento, tales como combustibles, alimentación, mantenimiento de vehículos y aeronaves, preparación de líneas de abastecimiento, etc.

Obviamente, para un Estado, la creación de un arma cibernética que se construye con el fin de obtener ventajas militares, políticas o simplemente anticiparse a los planes enemigos, siempre será más económico este camino.

> "Los ciberataques se han convertido en una alternativa real a las herramientas convencionales de inteligencia, muy especialmente debido a su bajo coste, a la dificultad de probar su autoría y al importante volumen de información que puede ser obtenido por esta vía. La mayor diferencia con relación a años pasados ha sido el incremento en los recursos en búsqueda de vulnerabilidades desconocidas y el aumento de la seguridad en estas operaciones" (Centro Criptológico Nacional, 2017, p. 29)

.

La atribución

Según Torres Soriano (2011) una de las característicos de la ciberguerra, son los problemas de atribución de responsabilidades entre los actores. Un ciber-ataque no siempre deja una huella que pueda ser rastreada hasta llegar al responsable. Asimismo, los procesos de investigación forense son complejos técnicamente y consumen una gran cantidad de tiempo y esfuerzo. Algunos de estos ataques se ejecutan utilizando cientos de miles de ordenadores repartidos por todo el planeta, los cuales han sido hechos «rehenes» temporalmente por los «ciber-guerreros», sin el conocimiento de sus propietarios. Utilizar este arsenal de «zombis» no solo puede ser una condición técnica para alcanzar el éxito, sino también una forma de enmarañar las responsabilidades y dificultar la respuesta. Aquí nace una nueva visión del mundo, frente a los componentes del campo de batalla, hoy en día además de analizar al adversario en su dispositivo, composición y fuerza, debe entenderse como una nueva disciplina el estudio de los ecosistemas digitales con que cuenta nuestro adversario, tareas como el ciberespionaje, la enumeración, y el escaneo deben ser palabras utilizadas en la nueva era de la guerra informática, el manejo de operaciones de información, denegación de servicio y la utilización de botnets[11] para obtener ventajas militares que permitan la toma de decisiones en operaciones en el mundo real.

"Sea como fuere, la atribución de este tipo de ataques es extraordinariamente difícil, todo ello sin olvidar que, en ocasiones, el mismo ataque es reivindicado desde diferentes partes." (Centro Criptológico Nacional, 2017).

Hay que entender que las operaciones combinadas entre lo virtual y lo real podrían dar una ventaja significativa en el logro de objetivos operacionales y estratégicos dice Ventre (2013). Por ejemplo se especula que el bombardeo producido en septiembre de 2007 por parte de la aviación israelí contra un reactor nuclear

[11] Botnet es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas.

en construcción en territorio sirio, fue posible por una acción previa de ciberguerra que engañó a los sistemas antiaéreos de Siria, e hizo posible la penetración en el espacio aéreo (Clarke, 2010).

Grandes retos se aproximan para los Estados, la regulación de este tipo de conflictos es algo que se ha venido discutiendo en la agenda internacional, no los explica Gonzalez (2010) algunos intentos se han realizado por estudiosos del tema como el manual de Tallin sobre el derecho internacional aplicable a los cyber warfare, escrito por un grupo Internacional de expertos independientes con el ánimo de examinar cómo aplicar las normas existentes de derecho internacional a esta nueva forma de guerra.

Por otro lado Wirtz (2017) realiza una analogía donde presenta un escenario de ciberataque con resultados catastróficos para los Estados Unidos y lo denomina como el Peral Harbor Cibernético, mencionando puntos de análisis sobre la estrategia que se debe tener para prevenir que este evento suceda; dentro de los puntos claves de su discusión se menciona una diferencia entre los actores poniendo como referencia a los Estados Unidos como una fuerza militar poderosa, influyente y persuasiva confrontada a un sinnúmero de enemigos con poder militar menor, pero con intenciones reales de afectar la infraestructura tecnológica militar de EEUU. Finalmente advierte que la mejor opción para hacer frente a un teatro de este estilo es incrementar su poder de persuasión disminuyendo a los posibles enemigos su interés en realizar esta afectación. Este autor nos muestra una diferencia en la preparación de un Estado frente a un escenario de ciberguerra, dado que todo su análisis va enmarcado a estrategia, táctica, métodos y procedimientos de toma de decisiones para enfrentarlo, asimismo frente a nuestra pregunta de investigación aporta que la Ciberdefensa debe verse como un conjunto de operaciones de carácter militar y no solo desde la parte técnica mediante soluciones como parches o mejoramiento de infraestructura, sino como un conjunto de actividades donde convergen las decisiones políticas, militares y tecnológicas.

Este artículo presenta una visión distinta, enmarcando la seguridad cibernética de un Estado como un conjunto de acciones lideradas por los militares, dado que las amenazas en la internet y sus efectos para un país tienen componentes adicionales a las tecnológicas y motivaciones especiales, para Wirtz (2017) si los técnicos son reacios a aceptar una solución basada en la estrategia, al problema de sorpresa cibernética, y por el contrario las respuesta se dan en el ámbito meramente técnico como parches y mejoras en la infraestructura sin ser orientadas por un contexto político – militar, de estrategia y contexto operacional, es probable que frente a los incentivos de la parte más débil no se pueda prevenir un Pearl Harbor Cibernético. Esto contrasta con lo que plantea Park (2016), donde no encuentra en la solución técnica la preparación del Estado de Corea frente a una amenaza de ciberguerra.

De acuerdo con Park (2016) el mundo cibernético en el que se encuentra inmerso el planeta, plantea serios problemas para la seguridad nacional de los Estados, mientras en algunas partes se presentan escaramuzas con afectaciones regionales, ya se han observado acciones de guerra a través de la red. Este autor realiza una comparación de la ley de prevención propuesto en la asamblea general de Corea del Sur en paralelo con la legislación vigente para prevención de ataques cibernéticos en Estados Unidos, Japón, China, Canadá, Francia y Noruega. Su conclusión no es preparación técnica sino por el contrario la creación de organismos interdisciplinarios e inter agénciales para prevenir y reaccionar.

En otra noción del fenómeno de la ciberguerra, Greathouse (2014) expone que las guerras en el futuro serán diferentes a las guerras del pasado, pero los teóricos clásicos siguen tan vigentes y sus postulados viables

al momento de intentar comprender este fenómeno, capaces de aportar información de valor para la comprensión sobre la naturaleza del conflicto y la política. De sus primeras observaciones se puede rescatar que, a diferencia de las armas del pasado, la tecnología necesaria para realizar actos de guerra cibernética no se encuentra restringida a algunos actores específicos, por el contrario, en la modernidad este tipo de ciberarmas están al alcance de todos sin importar edad, espacio geográfico, bando y demás, capaces de realizar actos que pueden parar una sociedad entera dependiente de la tecnología y la información. “Debido a que la guerra cibernética es poco convencional y la guerra asimétrica, naciones débiles en poder militar convencional también son propensos a invertir en ella como una forma de compensar las desventajas convencionales” (Geers, 2011).

Greathouse (2014) relaciona tres dimensiones dentro de la guerra cibernética, explicando que aun cuando es un mismo escenario existen diversidad de comportamientos dentro del mismo enfoque, ataques que se centran en objetivos estratégicos, ataques con objetivos técnicos y los de naturaleza política.

Así las cosas, manifiesta que los objetivos estratégicos son los que contienen sistemas de información, comunicaciones y seguridad civil; ataques técnicos son los que buscan el control de armas y comunicaciones militares, mientras que los de carácter político buscan desestabilizar el poder instaurado, generando incertidumbre, sabotaje y desinformación. (Saad et al. 2011) menciona que las armas cibernéticas incluyen virus, malware, denegación de servicio, espionaje y bloqueos.

Para poder evaluar los ataques cibernéticos (Schmitt 1999) propone la evaluación de seis criterios, los cuales son *gravedad, inmediatez, franqueza, invasividad, medición, presunción y legitimidad*; criterios acuñados con base en el derecho internacional, sin embargo a pesar de su importancia se considera como secundario al momento de definir una tipología de operaciones cibernéticas. Liaropoulos (2011) propone una amplia tipología, incluyendo espionaje cibernético, vandalismo web, denegación de servicio, y los ataques a la infraestructura crítica. Esto proporcionó un enfoque más práctico para definir tipos de operaciones cibernéticas, hay que tener en cuenta que la denegación de servicio en realidad puede estar dirigido a la infraestructura crítica.

La tipología propuesta parte desde la perspectiva basada en la gravedad e intensidad de cualquier ataque cibernético, para tal fin en la parte inferior de la pirámide se encuentra el vandalismo cibernético, actividades realizadas por algún troll o entusiasta descrito por Voutssas (2010) que realiza defacemen en una página oficial cambiando textos o imágenes que generen controversia. En segundo lugar, se ha puesto el espionaje cibernético definido como una acción de obtención de información que por sí misma no se encuentra disponible para su divulgación, sin embargo, a pesar de la gravedad e impacto que pueda tener un Estado con este tipo de actividad, su ubicación dentro de la topología es baja dada las consideraciones dentro del sistema internacional donde es permitido. En tercer lugar, se encuentra el crimen cibernético que a diferencia de los anteriores lleva inmerso un componente adicional y es el ánimo de lucro. Estos niveles anteriores no clasifican aun dentro de guerra cibernética; a continuación se determina que el siguiente escalón es la denegación de servicio, como su nombre lo indica es la actividad que realiza un atacante para afectar la disponibilidad de un activo de información, por tal motivo su implicación ya empieza a convertirse en acto de ciberguerra dependiendo de la intensidad y el objetivo de la denegación. Por ejemplo, no sería lo mismo si un estado realiza un ataque de DDOS sobre la infraestructura de comunicaciones de un Ejército, que si se realiza sobre un medio de comunicación. Su impacto para la seguridad del Estado varía aun cuando se utilice la misma técnica y el mismo método. La quinta categoría dentro de la topología es un ataque de destrucción de datos, software o

hardware que controla una parte importante de la infraestructura del adversario, esto podría incluir infraestructura eléctrica, gas, distribución de agua, sistemas bancarios, sector hidrocarburos, salud o conjunto de sistemas de comunicaciones. El último peldaño y de mayor impacto, es un ataque masivo diseñado para destruir los sistemas de red y datos totales de un actor, la diferencia del anterior consiste en la escala.

En la Ciberdefensa señala que si se fuera a plantear una estrategia de defensa en el ámbito de la guerra cibernética desde el principio sería defectuosa, ya que todas las maneras de defensa están en desventaja frente a la dominancia ofensiva, en segundo lugar, se refiere a que las defensas nunca van a ser perfectas ya sea por errores de programación, necesidad de aumentar privilegios o errores humanos. Por otro lado, la defensa puede ser efectiva para un Estado definiendo claramente que va a defender, pero se aborda un tema con muchas aristas, dado que si la protección del gobierno va enfocada únicamente a las redes del sector público, la empresa privada puede ser atacada impactando por carambola al Estado como un conjunto.

La postura frente a la disuasión genera discusión frente a que un Estado debería tener una capacidad de hacer daño a un adversario, y para lograr esto deben tenerse en cuenta los desarrollos tecnológicos, las políticas internas y la investigación y desarrollo como pilar fundamental, a través de alianzas con la empresa privada para la protección en conjunto.

Seguridad en el Ciberespacio con personal civil

El desarrollo de actividades de Ciberdefensa para un Estado no se puede llevar a cabo únicamente por parte del sector público, Axelrod (2015) describe cómo este teatro es diferente a otro tipo de confrontación con grandes avances en tecnología y en tácticas; afirma Palazzo (2014), tanto para la ciberdefensa como para la ciberseguridad; la empresa privada tiene grandes responsabilidades en la protección de su infraestructura, que de ser descuidada impactaría fuertemente al Estado Nación en conjunto. Menciona González (2010) que " la importancia de la seguridad en el ciberespacio ha llevado a los principales países a desarrollar estrategias, planes y legislación tendentes a prevenir y sancionar conductas delictivas, pero también a neutralizar ciberataques a su seguridad nacional", sumándole a ello que en la gran mayoría de las fuerzas militares se encuentran en un proceso de aprendizaje para enfrentar este tipo de combate, distinto a la visión clásica de la seguridad y defensa, y que requiere conocimientos técnicos específicos.

Nos explican Manchola, Suarez, & Herrera (2016, p.2) que en el proceso de realizar un delito informático, "se pueden visualizar tres pasos: • Elección de un objetivo. • Recopilación de información e investigación • Finalización del ataque. A través de tiempo, en Colombia, los delitos informáticos hechos por este tipo de hacker se volvieron un dolor de cabeza sobre todo para las entidades bancarias, quienes debido a la actividad de este grupo generan pérdidas millonarias, gracias principalmente a vulnerabilidades en los sistemas de información, el acceso a sus bases de datos de bancos por terceros y la clonación de tarjetas de crédito bancarias. Un ejemplo de estos delitos hechos por hackers de sombrero negro en entidades bancarias se da en la ciudad de Cali, en donde el delito se presenta por un mismo empleado de la entidad bancaria, que hurtaba dinero a los usuarios por medios informáticos utilizando la falsedad de documento privado."

Esto obliga a las Fuerzas Armadas a reinventarse en una misionalidad diferente, con actores distintos y variados, dentro de un espacio geográfico sin fronteras, con alta posibilidad de evolución y mutación; lo anterior obliga a los Estados a reclutar cibersoldados de carácter civil con experticia y experiencia en temas tecnológicos,

obviamente guiados por grandes estrategas conocedores del arte de la guerra, para lograr un equilibrio entre tácticas, técnicas y métodos, validando los riesgos de fuga de información y aceptándolos para así poder intervenir dentro del sistema internacional y ser actores con capacidad de disuasión, ataque y defensa. Una de las cosas importantes es que la guerra en el ciberespacio:

> "Es asimétrica. La barrera de entrada para la guerra cibernética es considerablemente inferior a la de la guerra convencional. La guerra cibernética requiere equipos conectados en red, y personas que a veces se hace referencia como "ciberguerreros". Los equipos incluyen los superordenadores para el agrietamiento, información encriptada, y el procesamiento de grandes cantidades de datos. Ciberguerreros incluyen los hackers y los defensores, traductores de idiomas extranjeros y analistas. La guerra cibernética no requiere un gran número de soldados, aviones, buques de guerra, misiles, equipos de logística, etc. Como tal, un pequeño grupo de personas cualificadas armados de PC y herramientas de apoyo, o un pequeño Estado-nación con cientos o miles de personas capacitadas con las computadoras y otras herramientas y personal de apoyo pueden atacar poderosos estados nacionales con un bajo riesgo de represalias." (Kim, 2012, p.324)

El riesgo con esta opción es la de reclutar contratistas civiles que cumplan labores dentro del concepto de operaciones militares en el ciberespacio y que dada su falta de formación militar, patriotismo y disciplina, puedan ser llaves abiertas para develar secretos de Estado que puedan generar riesgos políticos o militares con adversarios. El caso de mayor relevancia hasta el momento ha sido Edward Snowden, quien después de hacer parte de equipos dedicados al desarrollo de operaciones militares y de inteligencia en el ciberespacio, reveló a través de WikiLeaks métodos, procedimientos y datos de uso exclusivo del mando militar.

Conclusión

En este artículo se ha intentado revisar diferentes autores que han propuesto puntos de vista de cómo abordar la ciberdefensa en un Estado. Se observó que los componentes de una ciberguerra son variados y de difícil entendimiento, dado que desde un niño en su casa hasta un Estado con todo su poderío económico y tecnológico hacen parte de los actores que pueden ser víctimas o victimarios de incidentes o ciberataques. Por otro lado, se pudo evidenciar que aun con los mejores controles tecnológicos tanto en supervisión, control y análisis de eventos, siempre un humano interviene de dentro de este ecosistema digital.

Así pues, por medio del análisis y la interpretación de los resultados de investigaciones científicas, se determinó que los Estados no podrán cumplir con su misión de ciberdefensa de la nación sin el apoyo activo de la empresa privada y los civiles, dado que en este tipo de guerra el impacto de un ciberataque no solo afecta las instituciones públicas sino la sociedad como un todo. Por último, se puede concluir que las Fuerzas Armadas de un Estado que quiera fortalecer su seguridad en el ciberespacio deben reinventarse y profundizar en los esfuerzos de formación, capacitación, investigación y desarrollo de sus integrantes y determinar estrategias para actuar eficientemente en este nuevo escenario.

Las políticas internas deben ser ajustadas de acuerdo con sus necesidades de protección, entendiéndose que el escenario de ciberguerra además de ser real y de actualidad es una gran oportunidad para los países con recursos limitados en temas militares convencionales. Para convertirse en actor de primer nivel en el ciberespacio ya que una de las grandes características de este tipo de guerra es el bajo costo y la sencillez, la inversión no se medirá en cantidad de fusiles, tanques de guerra, aviones, buques sino en conocimiento y capacidades de desarrollo de ciberarmas efectivas.

Referencias

Arias-Cabarcos, P., Marin, A., Palacios, D., Almenarez, F., & Diaz-Sanchez, D. (2016). Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication. *IT Professional*, *18*(5), 34–40. https://doi.org/10.1109/MITP.2016.81

Armstrong, D. G., Kleidermacher, D. N., Klonoff, D. C., & Slepian, M. J. (2016). Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of “medjacking”. *Journal of Diabetes Science and Technology*, *10*(2), 435–438. https://doi.org/10.1177/1932296815602100

Axelrod, C. W. (2015). Cybersecurity and modern tactical systems. *CrossTalk*, *28*(6), 4–11.

Buzai, G. (2003). Cyberspace, new places, new positions. *Estudios Geograficos*, (250), 112–120.

Caro B., M. J. (2010). Alcance y ambito de la seguridad nacional en el ciberespacio. Recuperado a partir de file:///L:/descargas/Dialnet-AlcanceYAmbitoDeLaSeguridadNacionalEnElCiberespaci-3837251.pdf

Caruso, R. J., & Masters, M. (2014). Applying cyber risk management to medical device design. *Biomedical Instrumentation and Technology*, *48*(HORIZONS SPRING), 32–37. https://doi.org/10.2345/0899-8205-48.s1.32

Centro Criptológico Nacional,. (2017). *ciberamenazas y tendencias*. Recuperado a partir de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html

Chen, S., & Janeja, V. P. (2014). Human perspective to anomaly detection for cybersecurity. *Journal of Intelligent Information Systems*, *42*(1), 133–153. https://doi.org/10.1007/s10844-013-0266-3

Christakis, N. A., & Fowler, J. H. (2010). *Conectados, el sorprendente poder de las redes sociales y cómo nos afectan*. Santillana Ediciones Generales. Recuperado a partir de http://catedradatos.com.ar/media/2.-Christakis-Nicholas-A.-Conectados.pdf.pdf

Cimbala, S. J. (2016). Nuclear cyberwar and crisis management. *Comparative Strategy*, *35*(2), 114–123. https://doi.org/10.1080/01495933.2016.1176458

Clarke, R. (2010, junio). Ciberguerra. El Pearl Harbor Informatico. Recuperado el 10 de agosto de 2017, a partir de https://www.youtube.com/watch?v=-V5MDimfPc4

Elliott, K., Massacci, F., & Williams, J. (2016). Action, Inaction, Trust, and Cybersecurity’s Common Property Problem. *IEEE Security and Privacy*, *14*(1), 82–86. https://doi.org/10.1109/MSP.2016.2

Enamorado, J. J. (2013). *Manual de estudios estratégicos y seguridad internacional*. Plaza y Valdés España. Recuperado a partir de https://dialnet.unirioja.es/servlet/libro?codigo=549952

Everett, C. (2015). Cyberwar and protecting critical national infrastructure. *Computer Fraud and Security*, *2015*(11), 11–14. https://doi.org/10.1016/S1361-3723(15)30102-0

Gagnon, B. (2013). Cyberwars and cybercrimes. En *Technocrime: Technology, Crime and Social Control* (pp. 46–65). https://doi.org/10.4324/9781843925378

Garcia, G. L. (2005). El Ecosistema Digital modelos de comunicación, nuevos medios y público en internet. Recuperado el 11 de agosto de 2017, a partir de http://www.vinv.ucr.ac.cr/sites/default/files/divulgacion-ciencia/libros-y-tesis/ecosistema-digital.pdf

García, J. (2016). LA UNION EUROPEA Y LA OTAN EN EL MARCO DE LA NUEVA ESTRATEGIA GLOBAL DE LA UNIÓN EUROPEA. *Revista UNISCI / UNISCI Journal, Nº 42 (Octubre/October 2016*. https://doi.org/http://dx.doi.org/10.5209/RUNI.53794

García Rosales, D. F. (2015). The cardinal points of cyberspace in websites of Spanish political parties. *Opcion*, *31*(Special Issue 2), 425–443.

Geer, D. E. (2014). Personal data and government surveillance. *IEEE Security and Privacy*, *12*(4), 90–96. https://doi.org/10.1109/MSP.2014.73

Geers, K. (2011). Strategic Cyber Security. Recuperado a partir de https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf

Goel, S., & Hong, Y. (2015). *Cyberwar games: Strategic jostling among traditional adversaries* (Vol. 56). https://doi.org/10.1007/978-3-319-14039-1_1

Gonzalez, J. (2010). Dialnet-EstrategiasLegalesFrenteALasCiberamenazas-3837283.pdf. Recuperado el 14 de agosto de 2017, a partir de file:///L:/descargas/Dialnet-EstrategiasLegalesFrenteALasCiberamenazas-3837283.pdf

González, M. N. (2003). Capitulo I Definiciones y alcances del concepto de seguridad. *México y la Agenda Contemporánea de Seguridad Internacional: Un Estudio Sobre los Alcances del Uso del Concepto de Seguridad Humana*.

Gordon, K., & Dion, M. (2008). *PROTECTION OF 'CRITICAL INFRASTRUCTURE' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONALSECURITY*. Recuperado a partir de https://www.oecd.org/investment/investment-policy/40700392.pdf

Greathouse, C. B. (2014). Cyber war and strategic thought: do the classic theorist still matter. https://doi.org/10.1007/978-3-642-37481-4_2

Hurlburt, G. (2015). Cyberhuman security. *Computer*, *48*(5), 88–91. https://doi.org/10.1109/MC.2015.127

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and Cyberwars: Rebels with a cause?* https://doi.org/10.4324/9780203490037

Karatzogianni, A. (2008). *Cyber conflict and global politics*. https://doi.org/10.4324/9780203890769

Kim, W. (2012). On cyberwarfare. *International Journal of Web and Grid Services*, *8*(4), 321–334. https://doi.org/10.1504/IJWGS.2012.051522

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information and Communications Technology Law*, *23*(3), 220–237. https://doi.org/10.1080/13600834.2014.970432

Lucky, R. (2010). Cyber armageddon. *IEEE Spectrum*, *47*(9), 25. https://doi.org/10.1109/MSPEC.2010.5557511

Manchola, S. L., Suarez, G. H. C., & Herrera, B. O. E. (2016). Investigación sobre el hacker y sus posibles comienzos en la comunidad estudiantil. Caso Universidad Piloto de Colombia. En Rodriguez Y.A. (Ed.), *Euro Am. Conf. Telematics Inf. Syst., EATIS*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EATIS.2016.7520135

Marrero Travieso, Y. (2003). Cryptography and computer security element. *ACIMED*, *11*(6). Recuperado a partir de https://www.scopus.com/inward/record.uri?eid=2-s2.0-84899872463&partnerID=40&md5=ea53204f429fc52da4ec79985ea79e2b

Ministerio de Defensa de España. (2011). *La Evolución del Concepto de Seguridad*.

Mohammed, D. (2015). Cybersecurity compliance in the financial sector. *Journal of Internet Banking and Commerce*, *20*(1). Recuperado a partir de https://www.scopus.com/inward/record.uri?eid=2-s2.0-84939533853&partnerID=40&md5=12df4135111aed2bef2aa9810f85e57e

Palazzo, M. G. (2014). Cyberspace discourse practices of the young aesthetics and subjectivity in a blog case. *Tonos Digital*, (26). Recuperado a partir de https://www.scopus.com/inward/record.uri?eid=2-s2.0-84893682766&partnerID=40&md5=7603268b1373fae78eb93896fe67ea57

Park, D.-W. (2016). Analysis and comparison of regulations for national cybersecurity. *International Journal of Security and its Applications*, *10*(10), 207–214. https://doi.org/10.14257/ijsia.2016.10.10.19

Parra, I. D., & Mena, J. C. (2014). Geographical space and cyberspace in the 15m movement. *Scripta Nova*, *18*. Recuperado a partir de https://www.scopus.com/inward/record.uri?eid=2-s2.0-84897910579&partnerID=40&md5=9ae3aadbac110d5074b008c4ab3a54a9

Presidencia de los Estados Unidos. (2011). *international_strategy_for_cyberspace* (estratégia). Estados Unidos. Recuperado a partir de https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Quigley, K., Burns, C., & Stallard, K. (2015). "Cyber Gurus": A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, *32*(2), 108–117. https://doi.org/10.1016/j.giq.2015.02.001

Ruiz, J. L. S. (2002). La Gazeta de Antropologia: From local scarcity to global cyberspace. *Revista de Dialectologia y Tradiciones Populares*, *57*(1), 129–138.

Scheuerman, W. E. (2014). Edward Snowden: desobediencia civil para una era de vigilancia total. *Signos filosóficos*, *16*(32), 153–186.

Singer, P. W., & Friedman, A. (2014). *CYBERSECURITY AND CYBERWAR, "What every needs to know"*. Oxford University Press 198 Madison Avenue, New York, NY 10016. Recuperado a partir de file:///C:/Users/santi/Desktop/Cybersecurity_and_Cyberwar.pdf

Strawser, B. J., & Joy, D. J. (2015). Cyber Security and User Responsibility: Surprising Normative Differences. *Procedia Manufacturing*, *3*, 1101–1108. https://doi.org/10.1016/j.promfg.2015.07.183

Torres Soriano, M. R. (2011, marzo). Los dilemas estratégicos de la ciberguerra. Recuperado a partir de https://www.zotero.org/download/

Valenzano, A. (2014). Industrial cybersecurity: Improving security through access control policy models. *IEEE Industrial Electronics Magazine*, *8*(2), 6–17. https://doi.org/10.1109/MIE.2014.2311313

Vega Baeza, M. R., & Durán Medina, J. F. (2013). The cyberspace and the education. A pedagogy of the profitability? Weaknesses and strengths. *Estudios Sobre el Mensaje Periodistico*, *19*(SPEC. APR), 1077–1084. https://doi.org/10.5209/rev-ESMP.2013.v19.42192

Ventre, D. (2013). Cyberconflict: Stakes of Power. En *Cyberwar and Information Warfare* (pp. 113–244). https://doi.org/10.1002/9781118603482.ch4

Voutssas M, J. (2010). Documentary, digital and security information. *Investigacion Bibliotecologica*, *24*(50), 127–155.

Wirtz, J. J. (2017). The Cyber Pearl Harbor. *Intelligence and National Security*, *0*(0), 1–10. https://doi.org/10.1080/02684527.2017.1294379

Yang, Y., Gao, L., Yuan, Y.-B., McLaughlin, K., Sezer, S., & Gong, Y.-F. (2016). Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks. *IEEE Transactions on Power Delivery*, *PP*(99). https://doi.org/10.1109/TPWRD.2016.2603339

GESTIÓN DE RIESGOS
WWW.MASTERSECURITYCONSULTING.COM

MITIGA RIESGOS EN TU ORGANIZACIÓN

ANTES, DURANTE Y DESPÚES

IMPLEMENTA CONTROLES QUE REDUZCAN LOS RIESGOS

Auditorias e implementación de estándares en seguridad física, electrónica, de la información, realización de visitas domiciliarias, verificación de antecedentes, pruebas de lealtad, poligrafía pre-emleo y específica. Investigaciones.

MAS QUE CONSULTORES, SOMOS TUS ASESORES DE CONFIANZA

PREGUNTA POR LOS PAQUETES EMPRESARIALES Y KIT PYME TOTAL

contáctanos info@mastersecurityconsulting.com
+57 3165479295